REMARKS

In the office action mailed 05/02/05, claims 29-36 are rejected under various combinations of Lockhart, Ahmed, Latka, and Menzes.

Rejection of Claims Under 35 U.S.C. 103(a)

Re: Lockhart (US 5,841,873) and Ahmed (US 6,747,961)

Re: Lockhart, Ahmed, and Latka (US 5,646,996)

Re: Lockhart and Menezes (Handbook of Applied Cryptography)

Lockhart teaches the insertion of reference sequences into transmitted and encrypted data, and comparing such reference sequences to expected reference value at the receiver to determine cryptographic errors. Lockhart mentions checksums as the reference values (col. 4 lines 59-64) but fails to teach that the encrypted reference value is a checksum for a higher communication layer. Lockhart teaches that a checksum for higher layers should be added, if at all, after the reference value is added and after encryption of the sub-network packet:

"Additionally any link or transport check sums such as a CRC should be added after the reference value and encryption of the data packet. The preferred implementation for appending the reference value (205) to the data packet is provided by appending a 2-byte fixed length field containing the ASCII characters "EN" after the last byte of the data packet."

Regarding claim 42, there is nothing in Lockhart, Ahmed, or any of the other references to suggest calculating a checksum for a packet of a first communication layer and including the checksum in an encrypted packet of a second communication layer lower than the first communication layer.

Claim 37 recites that a checksum is extracted from a decrypted sub-network layer packet, a network layer checksum is calculated for a network layer packet comprising the

sub-network layer packet, and the checksum extracted from the decrypted sub-network layer packet is compared with the network layer checksum. Neither Lockhart nor any of the other references suggest such a technique.

Claim 41 recites a similar process on the encryption end.

Claim 38 recites that a network layer of a protocol stack detects the loss of stream cipher synchronization when the network layer checksum does not match the checksum extracted from the decrypted sub-network layer packet. Neither Lockhart nor any of the other references teach or suggest detecting loss of stream cipher synchronization by making a comparison of a checksum extracted from an encrypted sub-network packet with a checksum computed for a network layer packet. Nor do any of the references teach or suggest that the network layer checksum and the checksum extracted from the decrypted sub-network packet are both for a network layer data payload (e.g. see claim 39).

For at least these reasons, the claims should be allowed over the cited prior art.

Respectfully submitted,

Charles A. Mirho Reg. 41,199

112 W. 37th St., Vancouver, WA, 98660
Phone: 360-737-1748 Fax: 360-294-6426
Customer Number: 29586

Signature /Charles A. Mirho/_____ Date __08/01/05_____
Charles A. Mirho
Attorney for Applicant